



Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at <http://about.jstor.org/participate-jstor/individuals/early-journal-content>.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

THE GROUPS OF ORDER p^3q^β *

BY

F. N. COLE

§ 1. *Introduction.*

The researches of FROBENIUS† and BURNSIDE,‡ familiar to all students of the theory of groups, have established the non-existence of simple groups of orders pq^β and p^2q^β , p and q being different primes, and the consequent solvability of all groups of these orders. In the following paper I show that all groups of order p^3q^β are compound, and therefore also solvable. For convenience of reference I place at the beginning of the discussion the two following theorems of which repeated use is made in the subsequent reasoning :

I. *A simple group \mathfrak{G} of order $g = p^\alpha q^\beta$, p and q being different primes and $p > q$, cannot contain any subgroup \mathfrak{H} of order h whose index g/h in \mathfrak{G} is $< p^2$.*

In view of the results of FROBENIUS and BURNSIDE cited above, we assume that $\alpha > 2$.

The case $g/h < p$ is trivial. Here every group \mathfrak{A} of order p^α in \mathfrak{G} transforms every conjugate of \mathfrak{H} into itself and \mathfrak{G} is certainly compound. Again, for $g/h = p$, $h = p^{\alpha-1}q^\beta$, every subgroup of order $p^{\alpha-1}$ in \mathfrak{H} transforms \mathfrak{H} and therefore every conjugate of \mathfrak{H} into itself, and \mathfrak{G} is again certainly compound.

Suppose, now, that \mathfrak{K} is the largest subgroup of \mathfrak{G} that contains \mathfrak{H} and is less than \mathfrak{G} . Since \mathfrak{G} is simple, \mathfrak{K} is invariant under only those elements of \mathfrak{G} which are contained in \mathfrak{K} . The index g/k of \mathfrak{K} in \mathfrak{G} is $\equiv g/h$ and $> p$; \mathfrak{K} has g/k distinct conjugates in \mathfrak{G} .

1) Let $g/k = pq^i$ ($0 < i < p$), $k = p^{\alpha-1}q^{\beta-i}$. Having less than p^2 conjugates in \mathfrak{G} , \mathfrak{K} contains a subgroup of order $p^{\alpha-1}$ from every group \mathfrak{A} of order p^α in \mathfrak{G} . Every subgroup of order $p^{\alpha-1}$ of \mathfrak{K} is permutable with every subgroup \mathfrak{L} of order $g^{\beta-i}$ of \mathfrak{K} . \mathfrak{L} is invariant under a subgroup of \mathfrak{G} of order $g^{\beta-i+1}$, and this transforms \mathfrak{K} into at least one conjugate \mathfrak{K}' of \mathfrak{K} , different from \mathfrak{K} .

* Presented to the Society February 27, 1904. Received for publication February 1, 1904.

† FROBENIUS: Berliner Sitzungsberichte, 1895, p. 185; cf. Acta Mathematica, vol. 26 (1902), p. 198.

‡ BURNSIDE: Theory of Groups, p. 348. Cf. JORDAN, Liouville's Journal, ser. 5, vol. 4 (1898), pp. 21-26.

\mathfrak{K} and \mathfrak{K}' , having \mathfrak{L} in common, have no group of order p^{a-1} in common. Then \mathfrak{L} is permutable with two different groups of order p^{a-1} contained in the same group \mathfrak{A} of order p^a , and is therefore permutable with \mathfrak{A} . \mathfrak{L} and \mathfrak{A} generate a group of order $p^a q^{\beta-i}$ contained in \mathfrak{G} and having $< p$ conjugates in \mathfrak{G} .

2) Let $g/k = q^j (p < q^j < p^2)$, $k = p^a q^{\beta-j}$. As in 1), every conjugate of \mathfrak{K} contains a subgroup of order p^{a-1} from every group \mathfrak{A} of order p^a in \mathfrak{G} , and every subgroup \mathfrak{L} of order $q^{\beta-j}$ of \mathfrak{K} occurs also in a conjugate \mathfrak{K}' of \mathfrak{K} different from \mathfrak{K} . \mathfrak{K} and \mathfrak{K}' have in common the group \mathfrak{L} and a group of order p^{a-1} from every group \mathfrak{A} of \mathfrak{K} or \mathfrak{K}' ; their greatest common subgroup \mathfrak{D} is of order $p^{a-1} q^{\beta-j}$. All the conjugates of \mathfrak{D} in \mathfrak{K} or \mathfrak{K}' are obtained by transforming \mathfrak{D} by any group \mathfrak{A} of \mathfrak{K} or \mathfrak{K}' . Hence all the subgroups of order p^{a-1} in \mathfrak{D} are common to all the conjugates of \mathfrak{D} in \mathfrak{K} and \mathfrak{K}' . The subgroups of order p^{a-1} of \mathfrak{D} generate a group invariant in \mathfrak{K} and in \mathfrak{K}' , and therefore in a group \mathfrak{M} contained in \mathfrak{G} and containing \mathfrak{K} and $> \mathfrak{K}$. Then $\mathfrak{M} = \mathfrak{G}$, and \mathfrak{G} is compound.

II. If a simple group \mathfrak{G} of order $g = p^a q^\beta$, p and q being, as in I, different primes and $p > q$, contains a subgroup \mathfrak{H} of order $p^i q^j$ where $1 < q^{\beta-j} < p$, then \mathfrak{H} is contained in a subgroup \mathfrak{K} of \mathfrak{G} of order $p^{i+x} q^\beta$ ($x \geq 0$, $i + x < \alpha$).

Suppose that the largest group containing \mathfrak{H} and contained in \mathfrak{G} and $< \mathfrak{G}$ is \mathfrak{K} of order $k = p^{i+x} q^{j+y}$ ($j + y < \beta$); \mathfrak{K} is invariant under only those elements of \mathfrak{G} that are contained in \mathfrak{K} ; having $< p^{a-i-x+1}$ conjugates in \mathfrak{G} , \mathfrak{K} contains a subgroup of order p^{i+x} from every group \mathfrak{A} of order p^a in \mathfrak{G} . If $i + x = \alpha$, \mathfrak{G} is compound, by I. If $i + x < \alpha$ and $j + y < \beta$, a subgroup \mathfrak{L} of order q^{j+y} of \mathfrak{K} occurs in a conjugate \mathfrak{K}' of \mathfrak{K} different from \mathfrak{K} . \mathfrak{L} is permutable with two groups of order p^{i+x} from the same group \mathfrak{A} ; these with \mathfrak{L} generate a group \mathfrak{M} of order $p^{i+x+z} q^{j+y}$ ($z > 0$) containing \mathfrak{K} and contained in \mathfrak{G} and $< \mathfrak{G}$; but this is contrary to assumption.

A simple application of Theorem II is afforded by the groups of order $p^2 q^\beta$ ($p > q > 2$). A simple group of this order must contain p^2 subgroups \mathfrak{B} of order q^β , p of which have a common subgroup \mathfrak{D} of order q^r ($r > 0$) invariant in a group \mathfrak{D}' of order $p q^{r+s}$ ($s > 0$); $p^2 - 1$ is divisible by $q^{\beta-r}$, and $p - 1$ by q^s , hence $p - 1$ is divisible by $q^{\beta-r}$; \mathfrak{D}' is contained in a subgroup of order $p q^\beta$ of \mathfrak{G} . But then \mathfrak{G} is compound. The theorem controls also the case $q = 2$, except in the single event that $s = 1$ and $p + 1 = 2^{\beta-r-1}$.

§ 2. Preliminary treatment of the groups of order $p^3 q^\beta$.

A simple group of order $p^\alpha q^\beta$ ($p \leq q$) can occur only if $\alpha > 2\mu$, μ being the lowest index for which $p^\mu \equiv 1 \pmod{q}$.* For $\alpha = 3$, we can only take $\mu = 1$. A group \mathfrak{G} of order $p^3 q^\beta$ can be simple only if $p \equiv 1 \pmod{q}$; also $\beta > 2$, where $q^v \equiv 1 \pmod{p}$, therefore $q^\beta > p^2$.

* BURNSIDE, *Theory of Groups*, p. 345. Cf. FROBENIUS, *Acta Mathematica*, vol. 26 (1902), p. 194.

A simple group \mathfrak{G} of order $p^3 q^\beta$ must contain either p^2 or p^3 subgroups \mathfrak{B} of order q^β . Since $q^\beta > p^2$, the elements of these subgroups \mathfrak{B} cannot be wholly distinct in either case.

If \mathfrak{G} contains only p^2 subgroups \mathfrak{B} , and if two of these are so chosen that the order q^r of their greatest common divisor \mathfrak{D} is a maximum, then \mathfrak{D} is invariant in a subgroup \mathfrak{D}' of \mathfrak{G} whose order is $p^x q^{r+s}$ ($x = 1, 2; s > 0$) and which contains exactly p groups of order q^{r+s} . Here $p^2 - 1$ is divisible by $q^{\beta-r}$, therefore $p + 1 \equiv q^{\beta-r-1}$. (If $q \neq 2$, $p - 1$ is divisible by $q^{\beta-r}$, and \mathfrak{D}' has less than p^2 conjugates in \mathfrak{G} unless $x = 1$. For odd q , the discussion can be greatly simplified, as in the case of order $p^2 q^\beta$). Each of the $p^{3-x} q^{\beta-r-s}$ conjugate groups \mathfrak{D} occurs in exactly p of the groups \mathfrak{B} . If each of the p^2 groups \mathfrak{B} contains k of the groups \mathfrak{D} , the total number of the groups \mathfrak{D} is $p^2 k/p = p^{3-x} q^{\beta-r-s}$; hence $k = p^{2-x} q^{\beta-r-s}$. If now $x = 1$, each group \mathfrak{B} contains $p q^{\beta-r-s}$ groups \mathfrak{D} ; each of the latter is contained in $p - 1$ other groups \mathfrak{B} and no two of them occur together in any second group \mathfrak{B} . But there are only p^2 of the groups \mathfrak{B} and $p^2 < p q^{\beta-r-s} (p - 1) + 1$, unless $q^{\beta-r-s} = 1$, $r + s = \beta$. Then \mathfrak{D}' is of order $p q^\beta$, has exactly p^2 different conjugates in \mathfrak{G} , and therefore contains an element P of order p from every subgroup \mathfrak{A} of order p^3 in \mathfrak{G} .

Let \mathfrak{A} be any subgroup of order p^3 in \mathfrak{G} , and let \mathfrak{B} occur in \mathfrak{D}' ; having only p^2 conjugates in \mathfrak{G} , \mathfrak{B} is invariant under an element P of order p in \mathfrak{A} ; \mathfrak{B} is also permutable with a subgroup \mathfrak{A}_1 of order p in \mathfrak{A} not containing P . P transforms \mathfrak{D}' into a conjugate of \mathfrak{D}' different from \mathfrak{D}' and containing the group $P^{-1} \mathfrak{A}_1 P$, which is different from \mathfrak{A}_1 but is contained with \mathfrak{A}_1 in a subgroup \mathfrak{A}_2 of order p^2 of \mathfrak{A} . \mathfrak{B} is permutable with both \mathfrak{A}_1 and $P^{-1} \mathfrak{A}_1 P$ and therefore with \mathfrak{A}_2 ; \mathfrak{A}_2 and \mathfrak{B} generate a group of order $p^2 q^\beta$ contained in \mathfrak{G} and having only p conjugates in \mathfrak{G} .

Again, if $x = 2$ each group \mathfrak{B} contains $q^{\beta-r-s}$ of the groups \mathfrak{D} . The p groups \mathfrak{B} which have subgroups of order q^{r+s} in a same group \mathfrak{D}' contain $p(q^{\beta-r-s} - 1) + 1$ of the groups \mathfrak{D} , and these are transformed among themselves by every element of order p in \mathfrak{D}' . All the elements of order p in \mathfrak{D}' are therefore permutable with each of the remaining $p - 1$ groups \mathfrak{D} ; they generate a group which is invariant in p groups \mathfrak{D}' and therefore in a group \mathfrak{M} of order $p^{2+y} q^{r+s+t}$ ($y = 0, 1$) contained in \mathfrak{G} . If $y = 1$, \mathfrak{M} has at most $p + 1$ conjugates in \mathfrak{G} . And if $y = 0$, $t > 0$ and \mathfrak{M} has at most $p(p + 1)/q < p^2$ conjugates in \mathfrak{G} .

\mathfrak{G} must therefore contain p^3 sub-groups \mathfrak{B} . The maximum greatest common divisor \mathfrak{D} , of order q^r , of two of these is again invariant in a subgroup \mathfrak{D}' of order $p^x q^{r+s}$ ($x = 1, 2$) of \mathfrak{G} . Here $p^3 - 1$ is divisible by $q^{\beta-r}$, and $p - 1$, being divisible by q , is divisible by $q^{\beta-r-1}$ (in fact by $q^{\beta-r}$ if $q \neq 3$). Then, by the reasoning employed in the proof of Theorem II, if $r + s < \beta$, \mathfrak{D}' is contained in a subgroup of order $p^2 q^\beta$ of \mathfrak{G} . Hence $r + s = \beta$ and \mathfrak{D}' is of order

pq^β . Each group \mathfrak{D} is common to p groups \mathfrak{B} . If each group \mathfrak{B} contains k groups \mathfrak{D} , we have $p^3k/p = p^2$, hence $k = 1$; each group \mathfrak{D}' contains precisely one group \mathfrak{D} . Each group \mathfrak{B} occurs in only one group \mathfrak{D}' .

§ 3. *Final Investigation of the Groups of Order p^3q^β .*

Each of the p^3 groups \mathfrak{B} of \mathfrak{G} transforms among themselves the $p^3 - p$ conjugates of \mathfrak{B} not contained in the group \mathfrak{D}' in which \mathfrak{B} occurs. Let \mathfrak{D}' , and \mathfrak{B} in \mathfrak{D}' , be so chosen that a subgroup Δ common to \mathfrak{B} and a conjugate of \mathfrak{B} not contained in \mathfrak{D}' is of the largest possible order, and let this order be q^ρ . Then $q^{\beta-\rho}$ divides $p^3 - p$, and therefore divides $p^2 - 1$; $\rho > 0$, and in general $p > q^{\beta-\rho-1}$, the only exception occurring when $q = 2$ and $p + 1 = 2^{\beta-\rho-1}$. In this exceptional case $\beta - r = 1$, \mathfrak{D} is of order $2^{\beta-1}$.

The group Δ is common to two groups \mathfrak{B} from different groups \mathfrak{D}' . Δ is invariant under subgroups $\mathfrak{H}_1, \mathfrak{H}_2$ of order $q^{\rho+\sigma_1}, q^{\rho+\sigma_2}$ ($\sigma_1, \sigma_2 > 0$) of these two groups \mathfrak{B} . \mathfrak{H}_1 and \mathfrak{H}_2 cannot be contained in any subgroup of \mathfrak{G} of order $q^{\rho+\tau}$ ($\tau > 0$), for this subgroup would be common to two groups \mathfrak{D}' and therefore to two groups \mathfrak{B} contained one in each of these two groups \mathfrak{D}' . Δ is invariant in a subgroup Δ' of order $p^x q^{\rho+\sigma}$ ($x, \sigma > 0$) of \mathfrak{G} . Any subgroup of order p^x of Δ' transforms \mathfrak{D}' containing Δ into precisely p groups \mathfrak{D}' each containing Δ , for Δ cannot occur in all the p^2 groups \mathfrak{D}' . Δ' has one or more subgroups of order $q^{\rho+\sigma}$ common with each of these p groups \mathfrak{D}' , and no subgroup of order $q^{\rho+\tau}$ ($\tau > 0$) common with any other group \mathfrak{D}' . Hence Δ occurs in precisely p groups \mathfrak{D}' .

1) If $p > q^{\beta-\rho-1}$, or if $\sigma > 1$, then by Theorem II, Δ' is contained in a subgroup \mathfrak{M} of order pq^β of \mathfrak{G} (the order p^2q^β being inadmissible). \mathfrak{M} contains p groups \mathfrak{B} having Δ as their common subgroup; Δ is invariant in \mathfrak{M} , $\mathfrak{M} = \Delta'$, $\rho + \sigma = \beta$; and Δ has p^2 conjugates in \mathfrak{G} . If each group \mathfrak{D}' contains k groups Δ , then since each group Δ occurs in p groups \mathfrak{D}' we have $p^2k/p = p^2$, hence $k = p$.

If now two groups \mathfrak{D}' have more than one group Δ in common, their greatest common divisor \mathfrak{C} is of order pq^ρ and contains p groups Δ ; these are all the groups Δ contained in the two groups \mathfrak{D}' ; \mathfrak{C} is the smallest group that contains them; \mathfrak{C} is invariant in both groups \mathfrak{D}' and has $< p^2$ conjugates in \mathfrak{G} .

If no two groups \mathfrak{D}' have more than one group Δ in common, the p groups Δ contained in any group \mathfrak{D}' are distributed among $p(p-1)+1$ groups \mathfrak{D}' , and none of them occur in $p-1$ groups \mathfrak{D}' . All the elements of order p of a group \mathfrak{D}' are therefore permutable with each of $p-1$ other groups \mathfrak{D}' ; these elements of order p are common to p groups \mathfrak{D}' and are all the elements of order p of any of these p groups \mathfrak{D}' ; they generate a group invariant under the p groups \mathfrak{D}' and having $< p^2$ conjugates in \mathfrak{G} .

2) It remains to consider the special case $q = 2$, $p + 1 = 2^{\beta-\rho-1}$, $\sigma = 1$, $r = \beta - 1$. Let $\mathfrak{D}'_1, \mathfrak{D}'_2$ be two groups \mathfrak{D}' having a group Δ in common. Δ

cannot be the greatest common divisor of \mathfrak{D}'_1 and \mathfrak{D}'_2 , since either of the latter would then transform the other into $p2^{\beta-\rho} > p^2$ conjugates. The greatest common divisor \mathfrak{C} of \mathfrak{D}'_1 , \mathfrak{D}'_2 is therefore of order $p2^\rho$.

Suppose first that \mathfrak{C} contains only one group of order 2^ρ , that is, that Δ is invariant in \mathfrak{C} ; then Δ' contains \mathfrak{C} . If Δ' were of order $p2^{\rho+1}$, \mathfrak{C} would be invariant in Δ' and would contain every element of order p of Δ' ; whereas Δ' must contain an element of order p or p^2 which transforms \mathfrak{D}'_1 into \mathfrak{D}'_2 . Hence Δ' is of order $p^22^{\rho+1}$, and Δ has $p2^{\beta-\rho-1} = p(p+1)$ conjugates in \mathfrak{G} . If each group \mathfrak{D}' contains k groups Δ , we have $p^2k/p = p(p+1)$, $k = p+1$. Since Δ is invariant under an element p of \mathfrak{D}' , Δ is contained in the group \mathfrak{D} occurring in \mathfrak{D}' ; the $p+1$ groups Δ occurring in \mathfrak{D}' are conjugate in \mathfrak{D}' and are therefore all contained in \mathfrak{D} . No two groups Δ occurring in the same group \mathfrak{D}' can occur together in any second group \mathfrak{D}' . The p groups \mathfrak{D}' which have Δ in common, contain p^2+1 groups Δ , and do not contain any one of the remaining $p-1$ groups Δ . Δ' transforms among themselves the p^2+1 groups Δ occurring with Δ in groups \mathfrak{D}' , and transforms among themselves the remaining $p-1$ groups Δ . All the elements of order p or p^2 in Δ' are permutable with these $p-1$ groups Δ ; they all occur in p groups Δ' and are all the elements of order p or p^2 of each of these groups Δ' ; they generate a group invariant under p groups Δ' and having $< p^2$ conjugates in \mathfrak{G} .

The group \mathfrak{C} common to any two groups \mathfrak{D}'_1 and \mathfrak{D}'_2 must therefore contain p groups Δ . No group Δ is contained in a group \mathfrak{D} , for then Δ would be invariant in \mathfrak{C} . Since \mathfrak{D} is of order $2^{\beta-1}$, Δ has a subgroup \mathfrak{S} of order $2^{\rho-1}$ common with \mathfrak{D} . \mathfrak{S} is invariant in \mathfrak{C} , since \mathfrak{C} cannot have two groups of order $2^{\rho-1}$ common with \mathfrak{D} . \mathfrak{S} is also invariant under subgroups of order $2^{\rho+\tau_1}$, $2^{\rho+\tau_2}$ ($\tau_1, \tau_2 \equiv 0$) of \mathfrak{D}_1 and \mathfrak{D}_2 , and therefore under subgroups $\mathfrak{L}_1, \mathfrak{L}_2$ of order $p2^{\rho+\tau_1}$, $p2^{\rho+\tau_2}$ ($\tau_1, \tau_2 > 0$) of \mathfrak{D}'_1 and \mathfrak{D}'_2 respectively. \mathfrak{L}_1 and \mathfrak{L}_2 cannot both be contained in a group of order $p2^{\rho+\tau}$ containing \mathfrak{C} . The largest group \mathfrak{S}' contained in \mathfrak{G} and containing \mathfrak{S} as invariant subgroup is therefore of order $p^22^{\rho+\tau}$, where we must take $\tau = 1$, by virtue of Theorem II. \mathfrak{S}' transforms \mathfrak{D}' containing \mathfrak{S} into p groups \mathfrak{D}' containing \mathfrak{S} and has $p2^{\rho+1}$ elements in common with each of these p groups \mathfrak{D}' . \mathfrak{S} does not occur in any other group \mathfrak{D}'_i . For any group of order p^2 in \mathfrak{S}' could transform \mathfrak{D}'_i into only p groups \mathfrak{D}' ; \mathfrak{S}' would have an element P of order p common with \mathfrak{D}'_i ; \mathfrak{S} , being invariant under P , would be contained in \mathfrak{D}_i and would be invariant under a group of order 2^ρ of \mathfrak{D}_i ; this group of order 2^ρ would occur in \mathfrak{S}' and therefore in one of the p groups \mathfrak{D}' into which \mathfrak{S}' transforms \mathfrak{D}'_i ; and this would lead to the case already disposed of where \mathfrak{C} contains only one group Δ .

The group \mathfrak{S} has $p(p+1)$ conjugates in \mathfrak{G} and $p+1$ conjugates in each group \mathfrak{D}' . The $p(p+1)$ groups \mathfrak{S} are all different. The $p+1$ conjugates of \mathfrak{S} which occur in \mathfrak{D}' are conjugate in \mathfrak{D}' and are all contained in \mathfrak{D} . No

two groups \mathfrak{D}' can have two groups \mathfrak{S} in common, since this would again lead to the rejected case where \mathfrak{G} contains only one group Δ . The p groups \mathfrak{D}' which have \mathfrak{S} in common contains $p^2 + 1$ groups \mathfrak{S} . \mathfrak{S}' transforms these $p^2 + 1$ groups \mathfrak{S} among themselves. All the elements of order p or p^2 in \mathfrak{S}' are permutable with each of the remaining $p - 1$ groups \mathfrak{S} ; they generate a group invariant in p groups \mathfrak{S}' and having $< p^2$ conjugates in \mathfrak{G} .

COLUMBIA UNIVERSITY,
January, 1904.
